FACT SHEET

IDEM's Y2K Enforcement Policy

August, 1999

What is the Y2K Computer Problem?

The Year 2000 computer problem, known as Y2K or the Millennium Bug, arises from the widespread use of a two-digit field instead of four to represent the year in computer databases, software applications, and hardware chips (for example 06/18/85). On January 1, 2000, computers may recognize "double zero" not as 2000 but as l900. The glitch could cause date sensitive items to operate unpredictably or stop running. There are other upcoming dates that could cause computer-related problems, however January 1, 2000 has the greatest potential. Together these dates are termed the Y2K bug.

Why is this a problem for IDEM?

IDEM's mission is to protect public health and the environment. Information technology is an essential component in this protection. If businesses or communities do not handle Y2K properly, the problems could have serious ramifications on the preservation and protection of the environment and health. Serious effects could occur, such as accidental contamination of drinking water, the release of harmful pollutants into the air, and the disruption of basic services to the public.

What is IDEM's Enforcement Policy for violations that occur due to Y2K problems?

IDEM's Y2K Enforcement Policy is primarily focused on providing a climate to encourage Y2K testing in advance of the millennium. Regulated facilities who test in advance of the Y2K dates are encouraged to utilize any existing regulatory or permit procedures that may apply and provides a process for testing. For example, IDEM's Self-Disclosure and Environmental Audit Policy may be utilized. If no regulatory or permit procedures apply, or can't be done in a timely manner, then the Y2K Enforcement Policy may be used.

Under this policy, IDEM expects to exercise its discretion to waive 100% of the civil penalties that may otherwise apply and to recommend against criminal prosecution for violations resulting from testing **IF** the facility meets **all** of the following criteria:

- Test protocols were designed in advance of the testing period;
- Y2K testing was the cause of any potential violations where penalty waiver is sought;
- The testing was needed to assess Y2K compliance status or test the effectiveness of Y2K modifications, was conducted before the Year 2000, and are a part of a comprehensive testing program to correct all Y2K problems;
- The tests were conducted for the shortest possible period of time, not to exceed 24 hours in duration;
- Tests to determine Y2K compliance of existing equipment were made without modifications;
- Violations did not create a potentially imminent and substantial endangerment to human health or the environment;
- All violations ceased at the end of the test or were corrected within 24 hours after the test;
- The facility quickly remediated any releases or other adverse consequences as specified by IDEM, and;
- The facility reported violations (including violations required to report by law and those not

legally required to report) to IDEM within 30 days and no later than February 1, 2000.

What can the regulated community do to help solve the Y2K problem?

Many businesses and communities have been working toward Y2K compliance, but many businesses and communities, especially smaller entities, have had more difficulty. IDEM strongly encourages all business and communities to check for Y2K compliance. IDEM recommends businesses complete six items to help ensure normal operations on January 1, 2000. These efforts should already be underway.

 # Awareness
Raise awareness and establish a Y2K project team in your organization. Partner with other groups and share information to resolve this problem. Prepare a Y2K budget.

 # Assessment
Inventory information systems and equipment. Test computer systems and equipment for Y2K compliance.

 # Repair/Correction
Once the problem areas have been identified, correction of the systems should occur. This can involve modification, repair or replacement of systems or components. There are diagnostic programs available as well as consulting firms and computer specialists that can assist in making the necessary corrections. Some of this information is also available on Year 2000 Web sites.

 # Contingency Plans
As a back up measure, all systems should have a contingency plan to deal with unforseen problems and emergencies. Among other things, these plans should address how systems will operate while a Y2K fix is developed. The plan should be revised after the testing/validation phase.

 # Testing/Validation
Run validation tests on the systems/equipment to make sure the problems are solved. Tests should be run as soon as possible to allow time for any additional changes. Independent verification of the test may be appropriate in some cases.

 # Implementation
Once the systems are modified to operated correctly, they should be retested and re-validated. Then they are ready for implementation.

Where Can I Get More Information?

On the State Year 2000 web site at http://www.ai.org/dpoc/y2k/y2khome.htm, you will find how Y2K affects state agencies and how the State of Indiana is addressing Y2K. Links to other Y2K information are available.

At the US Environmental Protection Agency at, http://www.epa.gov/year2000. Among many items, you will find a tool kit that contains a list of all Y2K potential problematic dates, and various business sectors' fact sheets.

The State Emergency Management Agency has Y2K recommendations at:
http://www.state.in.us/sema/y2k/index.html
or call: (317) 232-3980.

For the full IDEM Y2K Enforcement Policy please visit our web site at:
http://www.state.in.us/idem/oe/nrp/y2k.html